Team 11 Trustworthy Modules STRIDE Analysis

As a service provider and user of the internet, the service we provide will be under constant threat of security breach. As such, we have constructed a security analysis of our system using the STRIDE method (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege), with the goal of exposing the potential downfalls of our system. To complete this analysis, we have assumed that a supposed attacker has absolutely every resource at their disposal, in a worst-case scenario type of event.

Spoofing: Supposing an attacker has permissions of an internal user, they would be able to see modules produced by ACME, which would expose ACME to the various problems associated with people being able to see code only intended for private usage.

Tampering: As of current, our system is essentially immune to tampering. The only tampering that could be done is adding more modules to be tracked, so just based off of the intended functionality of our system, there is provided safety from tampering.

Repudiation: Repudiation is something that could easily happen within our system as there is currently not a way to track who is responsible for changes, so users could easily deny their usage but the reasons for doing so would make this attack extremely unlikely.

Information Disclosure: By using our system, the information that could potentially be disclosed would mostly pertain to private code bases that are being graded using our system. As such, this attack is similar to the Spoofing category in that the potential risks would be that a user is able to leak private code.

Denial of Service: Currently, we have no way to handle large amounts of traffic, meaning that our system is excessively vulnerable to Denial of Service attacks. This threat is partially mitigated by Google's Cloud Platform naturally having some defenses against this, however our system in and of itself could benefit from the additional security of better support for large numbers of users.

Elevation of Privilege: If a user were able to elevate their privileges they would eventually be able to see private repositories being graded in our system, but currently our system does not support many forms of privilege anyways, so currently this threat is very low but it will eventually be something to worry about.